PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04N 7/167, H04H 1/00 — A1

(11) International Publication Number: WO 91/12693

(43) International Publication Date: 22 August 1991 (22.08.91)

(21) International Application Number: PCT/GB91/00228

(22) International Filing Date: 14 February 1991 (14.02.91)

(30) Priority data:
9003325.9 14 February 1990 (14.02.90) GB

(71) Applicant *(for all designated States except US)*: ENFRANCHISE SIXTY LIMITED [GB/GB]; St John's Innovation Centre, Cowley Road, Cambridge CB4 4WS (GB).

(72) Inventor; and

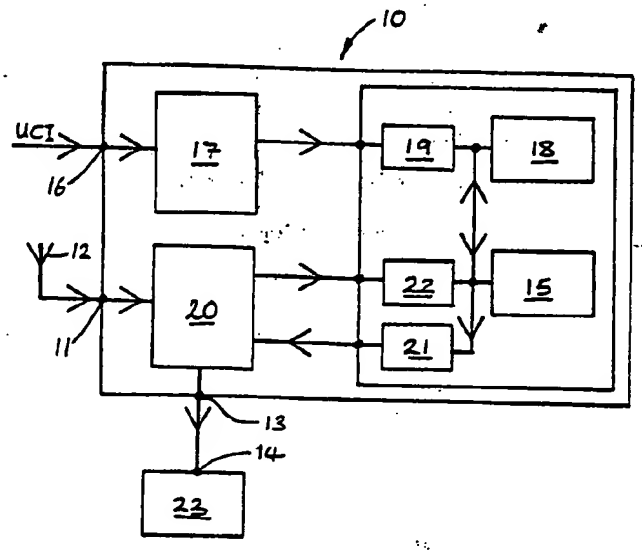
(75) Inventor/Applicant *(for US only)* : HAWTHORNE, William McMullan [GB/GB]; Kenmare, Bramerton Road, Surlingham, Norwich, Norfolk NR14 7DE (GB).

(74) Agent: JONES, William; Willow Lane House, Willow Lane, Norwich, Norfolk NR2 1EU (GB).

(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CM (OAPI patent), DE, DE (European patent), DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), GR (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MR (OAPI patent), MW, NL, NL (European patent), NO, PL, RO, SD, SE, SE (European patent), SN (OAPI patent), SU, TD (OAPI patent), TG (OAPI patent), US.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS AND METHOD FOR CONTROLLING ACCESS TO BROADCAST SIGNALS



(57) Abstract

A method of controlling access to a broadcast signal characterised by the method comprising: issuing a first substantially unique key to each intending user; issuing to each user to be allowed access a message enciphered by use of the key unique to that user so as to permit local deciphering of the ciphered message by use of the issued first key to constitute a second key; and broadcasting a signal enciphered by use of said second key so as to permit local deciphering of the ciphered signal by use of the second key. The invention also provides a television receiver control apparatus for use with the above method.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland			SN	Senegal
CI	Côte d'Ivoire	KR	Republic of Korea	SU	Soviet Union
CM	Cameroon	LI	Liechtenstein	TD	Chad
CS	Czechoslovakia	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

APPARATUS AND METHOD FOR CONTROLLING ACCESS TO BROADCAST SIGNALS

Field of the Invention

This invention relates to the control of access to broadcast signals, particularly, but not exclusively, video services such as television programmes and broadcast data services such as financial and medical information services. Such access control and regulation is of use in ensuring payment for selected broadcast services by subscribing users.

Background to the Invention

The control of access presents two problems. The first problem is to provide a method of distorting, scrambling or otherwise enciphering the broadcast signal so that it becomes substantially meaningless to a non-subscribing viewer, and at the same time the method should be strong in terms of irreversibility so that it becomes very difficult or uneconomic to manufacture unauthorised or pirate devices for recreating the plain signal. A number of suitable ciphers are known to those skilled in the communication arts. The cipher should preferably be a key symmetric cipher.

The second problem is to provide a method and apparatus for ensuring that the user cannot continue to gain access after his subscription expires or his contract with the broadcasting agency ceases to be in force. This problem is more difficult because the user has already been provided with a control device or decoder for use during his subscription period and may decline to return

his decoder, necessitating expensive legal proceedings. Even if the cipher is changed at the end of each subscription period, the decoder itself constitutes a structure for reverse engineering by a potential manufacturer of pirate devices who will assume that the cipher changes will be trivial. The problem is to provide such a control device which will for all practical purposes be useless after expiry of a subscription but which can be rendered operative again should the subscription subsequently be renewed.

An object of the present invention is to provide a method and apparatus which allows solution of this technical problem.

Summary of the Invention

According to the present invention in one aspect there is provided a method of controlling access to a broadcast signal characterised by the method comprising:

issuing a first substantially unique key to each intending user;

issuing to each user to be allowed access a message enciphered by use of the key unique to that user so as to permit local deciphering of the ciphered message by use of the issued first key to constitute a second key; and

broadcasting a signal enciphered by use of said second key so as to permit local deciphering of the ciphered signal by use of the second key.

In another aspect the invention provides a method of gaining local access to a broadcast signal characterised by the method comprising:

locally storing a first substantially unique key;

locally storing first and second deciphering algorithms;

locally entering a ciphered message which has been ciphered at another location by use of said first key;

deciphering said ciphered message by use of said local first key and the first algorithm to constitute a second key; and

receiving and deciphering a ciphered broadcast signal by use of said second key and the second algorithm, said broadcast signal having been ciphered at another location by use of a second key.

In a further aspect the invention provides television receiver control apparatus characterised in that the apparatus comprises:

memory means for storing a first substantially unique key;

first means for storing a first deciphering algorithm;

second means for storing a second deciphering algorithm;

data entry means for entry of a ciphered message by a user seeking access to a broadcast video signal;

first deciphering means activated by said first key to decipher said ciphered message by use of said first deciphering algorithm whereby the deciphered message constitutes a second key; and

second deciphering means activated by said second key to decipher a received ciphered broadcast video signal by use of said second deciphering algorithm.

The present invention also includes within its scope a method of controlling access to a broadcast signal, and independently a

method of gaining local access to a broadcast signal, substantially as described herein with reference to, and as illustrated in, the accompanying drawings. Furthermore, the invention includes within its scope television receiver control apparatus substantially as described herein with reference to, and as illustrated in, the accompanying drawings.

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings; in which:

Brief Description of the Drawings

Figure 1 is a block circuit diagram of an access control unit according to the invention, for use with a subscriber's television receiver; and

Figure 2 is a flow chart of operation of a control method according to the invention.

Description of the Preferred Embodiment

Figure 1 shows a control unit 10 for use with a television receiver 23 to control access to a video signal which is broadcast in ciphered form. The control unit has an input 11 connected to the local TV antenna 12, and an output 13 connected to the television receiver antenna input socket 14. The control unit is adapted to decipher a ciphered video signal received at its input 11 and to provide a deciphered plain video signal at its output 13.

The control unit 10 contains memory means 15 which includes a memory for storing a first key termed the Message or M-cipher key, and memories for storing first and second deciphering algorithms referred to as the M and V deciphering algorithms respectively. The memory is suitably an integrated circuit chip. Before delivery to the user the memory chip is primed with the M and V deciphering algorithms and with a substantially unique M-

cipher key. The M-cipher key is suitably in the form of a serial number in the range of from 1 to 1,000,000,000,000 whereby the system can create up to a million million different ciphertext messages from a single plain text message and can thereby accommodate a million million subscribers.

The M-cipher is a key symmetric message cipher, i.e a cipher which, in response to activation by a key, converts an intelligible stream of letters and numbers, i.e the message, into an unintelligible stream, and which also operates in reverse to convert the unintelligible stream back to the intelligible stream upon activation by an identical key.

The V-cipher is a key symmetric video cipher which applies the same properties of key activation and reversibility to a video signal. The broadcast video signal is ciphered by use of the V-cipher key before transmission. The ciphered broadcast video signal is thus common to all subscribers and there is no requirement to broadcast individualised coded video signals.

Upon payment or renewal of his subscription a user in possession of a primed control unit receives a ciphered message to allow him to enable the control unit. The ciphered message is referred to as Unique Customer Information or UCI. Each message is in numerical form and consists of M-cipher ciphertext of the V-cipher key for the next broadcasting period from the pertinent broadcasting organisation. Each UCI is substantially unique because it has been created by using the M-cipher key specific to each subscriber.

The control unit 10 is provided with data entry means 16 connected to a data input circuit 17 so that the user can enter his UCI message. The data entry means can be a numerical keyboard or keypad, an alphanumeric keyboard, a slot to accept a coded card, a modem connected to a public telephone line or any other convenient arrangement. The UCI message can be represented in print and sent to the subscriber by mail who then

enters the number on the keyboard. The UCI message can alternatively be embodied in a punched card, a magnetic strip card, a dumb memory card containing memory but no processor, or a smart memory card containing both a memory and a processor. These cards can be sent by mail to the user who then inserts the card in the slot in the control unit and the UCI message is transferred by means appropriate to the type of card, as known to those in the art.

When the UCI message is embodied in print or on a card it can be sent by mail or the subscriber can apply to a vending station. An alternative arrangement which offers greater flexibility is for the control unit to receive the UCI message through a modem or other device coupled to a public telephone line, in response to a telephoned request by the subscriber. This would allow an accounting and management system to be automatically linked to the existing telephone account billing system, and will also permit great flexibility in the terms and periods for each UCI message.

When the UCI message is entered into the control unit it is deciphered by use of the unique M-cipher key stored in the local memory 15 in accordance with the M-deciphering algorithm also stored in the local memory 15, whereby to constitute the V-cipher key. The deciphering is effected by a processor 18 connected through a latch 19 to the data input circuit 17. Because the UCI message is unique to that subscriber he cannot make use of any UCI message supplied to any other subscriber and nor can the other subscriber make use of the first subscriber's UCI message. If any such inappropriate UCI message is entered into a control unit it cannot operate to generate the necessary V-cipher key. If the subscriber ceases payment and the subscription period expires, his previous UCI message and the control unit become useless since a fresh UCI message is then necessary for the next period.

The V-cipher key generated from the UCI by the M-cipher key and the M-algorithm is common to all users and is specific to a predetermined pay time period. In a very simple arrangement, a subscriber is issued with a data card once a year to give him blanket access to all channels broadcast in V-cipher form. This would replicate the present contractual position with regard to the BBC annual licence fee. The invention is however adaptable to numerous other possibilities at various levels of selective viewing. For example broadcast programmes can be categorised as sport, news, entertainment, features etc., and the pay period can be 3 months, 6 months etc., and can be specific to one or more selected broadcast channels. At its most flexible a particular UCI message could cover simply a single programme for which there is high demand such as a World Cup football final.

By way of example a UCI message in plaintext, i.e before M-ciphering, might be the number sequence 329466219. The portion 329 is a broadcasting station identifier, the portion 46 is a time period identifier, and the portion 6219 is the V-cipher deciphering key applicable to V-ciphered broadcasts to take place in the identified time period 46. This example requires the station identifier and the time period to be broadcast together with the ciphered broadcast video signal. This can be accomplished by any of the various methods known to those in the art, for example within the videotext lines, in the lines at the extremities of the active picture area, in digital form within the line or frame synchronisation signals, or modulated on to a sub-carrier transmitted together with the video signal. The broadcast video signal including the station identifier and the time period is common to all subscribers, and no individualised signals are broadcast.

In operation the control unit locally generates the necessary V-cipher key and extracts the station identifier and the time period from the UCI, and then stores these items in memory within memory means 15 for on-line use. When the user wishes to view a

programme broadcast in V-cipher form, the signal captured by his local antenna 12 is supplied through input 11 to a video processor 20. The processor 20 deciphers the ciphered video signal on-line using the V-cipher key and in accordance with the V-deciphering algorithm also stored in memory 15 and supplied to and from the processor 20 through latches 21 and 22. The deciphered plain video signal is fed out from output terminal 13. The processor 20 is enabled to operate only if the station identifier and the time period broadcast with the video signal coincide with the station identifier and time period extracted from the UCI message and currently stored for comparison in memory 15.

Figure 2 shows a flow chart which summarises a method according to the invention using relatively short number sequences as examples.

Figure 2 may be understood using the identification table that follows:

IDENTIFICATION TABLE

24	Broadcasting station
24.1	Transmits programme enciphered with V-key = 7093
25	Control centre
25.1	Inputs V = 7093 into M-cipher
25.2	Creates unique UCI messages as M-cipher text of 7093 using M-keys 9618; 2903; 7854
25.3	Unique UCI is sent to each subscriber
26	Subscriber 1

26.1 M-cipher key = 9618

26.2 M-cipher deciphers 3214; V-key = 7093

26.3 V-cipher deciphers broadcast

27 Subscriber 2

27.1 M-cipher key = 2903

27.2 M-cipher deciphers 5587; V-key = 7093

27.3 V-cipher deciphers broadcast

28 Subscriber 3

28.1 M-cipher key = 7854

28.2 M-cipher deciphers 9016; V-key = 7093

28.3 V-cipher deciphers broadcast

The numerals 3214, 5587 and 9016 in Figure 2 are the unique UCI's sent to each subscriber.

Briefly the control centre 25 selects 7093 as the V-cipher key which will be employed in the next broadcasting time period (see 25.1). The centre 25 then uses the M-ciphering algorithm on 7093 successively in combination with each unique M-cipher key to create the unique UCI messages for each subscriber (see 25.2). For example, subscribers 1, 2 and 3 (see 26, 27 and 28 respectively) have been allotted M-cipher keys 9618; 2903; and 7854 (see 26.1, 27.1 and 28.1 respectively), and have control units 10 (see Figure 1) respectively primed with these keys. The UCI messages for subscribers 1, 2 and 3 might then be 3214; 5587; and 9016, as shown in Figure 2.

The station identifier and the time period identifier and any other relevant information are added to the UCI messages which are then mailed or otherwise transmitted to the individual subscribers. Subscriber number 1 inputs UCI message 3214 and his control unit uses its unique local M-cipher key 9618 to decipher 3214 to constitute the original V-cipher key 7093 (see 26.2). Similarly the control unit of subscriber number 2 uses its unique M-cipher key 2903 to decipher 5587 to constitute the same original V-cipher key 7093 (see 27.2), and the control unit of subscriber number 3 uses its unique M-cipher key 7854 to decipher 9016 to constitute the same original V-cipher key 7093 (see 28.2).

It will be appreciated that no M-cipher key information is transmitted with the UCI messages and that the M-cipher keys of two subscribers bear no relationship to one another. The common V-cipher key 7093 generated in each subscriber's control unit can then decipher a programme broadcast in V-enciphered form (see 24.1) in the relevant time period as described above (see 26.3, 27.3 and 28.3 respectively).

It will also be appreciated by those skilled in the art that, although the invention has been particularly described in relation to video or television signal scrambling, it is also applicable to the encryption of other forms of broadcast service.

CLAIMS:

1. A method of controlling access to a broadcast signal characterised by the method comprising:

issuing a first substantially unique key to each intending user;

issuing to each user to be allowed access a message enciphered by use of the key unique to that user so as to permit local deciphering of the ciphered message by use of the issued first key to constitute a second key; and

broadcasting a signal enciphered by use of said second key so as to permit local deciphering of the ciphered signal by use of the second key.

2. A method of controlling access to a broadcast signal according to Claim 1 characterised in that the ciphered message is embodied in a punched card, a magnetic strip card, a dumb memory card or a smart memory card.

3. A method of gaining local access to a broadcast signal characterised by the method comprising:

locally storing a first substantially unique key;

locally storing first and second deciphering algorithms;

locally entering a ciphered message which has been ciphered at another location by use of said first key;

deciphering said ciphered message by use of said local first key and the first algorithm to constitute a second key; and

receiving and deciphering a ciphered broadcast signal by use of said second key and the second algorithm, said broadcast signal having been ciphered at another location by use of a second key.

4. A method of gaining local access to a broadcast signal according to Claim 3 characterised in that the ciphered message is embodied in a punched card, a magnetic strip card, a dumb memory card or a smart memory card.

5. Television receiver control apparatus characterised in that the apparatus comprises:

memory means for storing a first substantially unique key;

first means for storing a first deciphering algorithm;

second means for storing a second deciphering algorithm;

data entry means for entry of a ciphered message by a user seeking access to a broadcast video signal;

first deciphering means activated by said first key to decipher said ciphered message by use of said first deciphering algorithm whereby the deciphered message constitutes a second key; and

second deciphering means activated by said second key to decipher a received ciphered broadcast video signal by use of said second deciphering algorithm.

6. Television receiver control apparatus according to Claim 5 characterised in that the data entry means is a numerical keyboard or keypad, a slot to accept a coded card, or a modem connected to a telephone line.

FIGURE 1

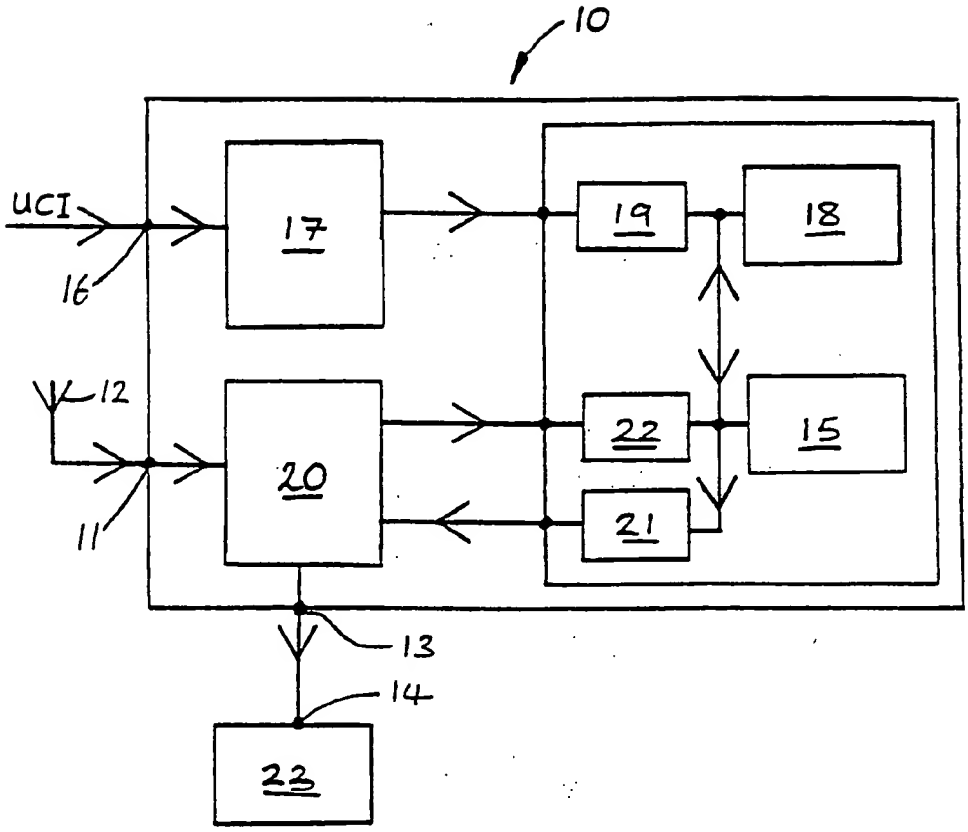
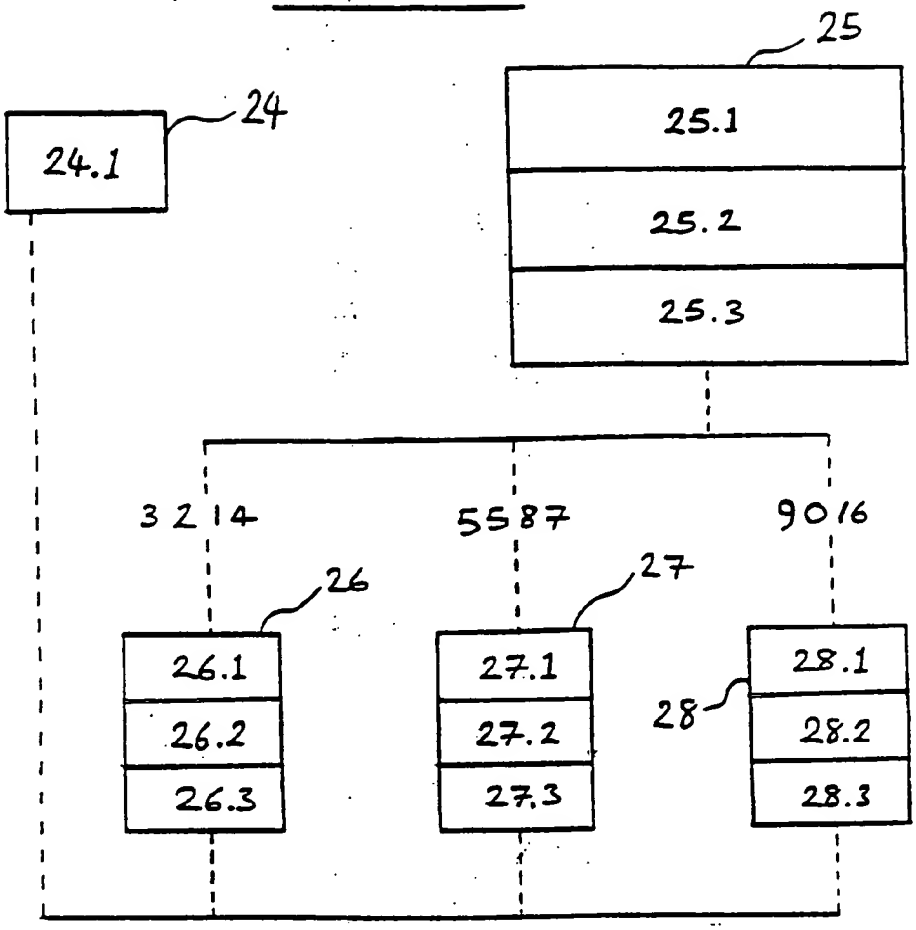


FIGURE 2


25
24
24.1
25.1
25.2
25.3
3214
5587
9016
26
27
28
26.1
26.2
26.3
27.1
27.2
27.3
28.1
28.2
28.3

INTERNATIONAL SEARCH REPORT

International Application No PCT/GB 91/00228

I. CLASSIFICATION OF SUBJECT MATTER (If several classification symbols apply, indicate all)[6]

According to International Patent Classification (IPC) or to both National Classification and IPC

Int.Cl. 5 H04N7/167 ; H04H1/00

II. FIELDS SEARCHED

Minimum Documentation Searched[7]

Classification System	Classification Symbols
Int.Cl. 5	H04N ; H04H

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched[8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT[9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No.[13]
X	GB,A,2132860 (BRITISH BROADCASTING CORP.) 11 July 1984 see page 1, lines 17 - 42 see page 2, lines 30 - 43 ---	1-6
X	EP,A,0155762 (M/A-COM GOVERNMENT SYSTEMS) 25 September 1985 see page 3, line 5 - page 5, line 25 ---	1
X	WO,A,8607224 (SCIENTIFIC ATLANTA) 04 December 1986 see page 6, lines 6 - 25 ---	1
A	WO,A,8606240 (PAYTEL LTD) 23 October 1986 see page 7, line 25 - page 13, line 8 ---	1, 2, 6
X,P	EP,A,0375539 (LABORATOIRE EUROPEEN DE RECHERCHES ELECTRONIQUES AVANCEES) 27 June 1990 see the whole document ---	1

* Special categories of cited documents : [10]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
21 MAY 1991	- 4. 07. 91
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	M. PEIS M. Peis

Form PCT/ISA/210 (second sheet) (January 1985)

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON INTERNATIONAL PATENT APPLICATION NO.

GB 9100228
SA 44572

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 13/06/91

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
GB-A-2132860	11-07-84	None		
EP-A-0155762	25-09-85	US-A-	4634808	06-01-87
		AU-B-	566316	15-10-87
		AU-A-	3954085	19-09-85
		CA-A-	1225458	11-08-87
		JP-A-	61016643	24-01-86
WO-A-8607224	04-12-86	AU-A-	5812086	24-12-86
		EP-A-	0222818	27-05-87
		JP-T-	62503066	03-12-87
WO-A-8606240	23-10-86	EP-A-	0218703	22-04-87
EP-A-0375539	27-06-90	FR-A-	2641152	29-06-90
		CA-A-	2006459	23-06-90
		WO-A-	9007845	12-07-90